НАО «Восточно-Казахстанский технический университет имени Д. Серикбаева»

Дисциплина «Теоретико-числовые методы в криптографии»

ПРАКТИЧЕСКАЯ РАБОТА 1

ДЕЛИМОСТЬ И ОСТАТКИ

Методические указания и задание к выполнению

Аудиторная нагрузка: 1 академический час. Сначала изучите методичку с примерами, затем переходите к индивидуальным заданиям. Программные примеры предназначены для подготовки и самостоятельной проверки.

1 Цель работы

Цель работы — научиться обосновывать делимость, правильно находить остатки положительных и отрицательных целых чисел и использовать их в простых вычислительных задачах. Перед выполнением необходимо изучить лекцию 1, особенно доказательство единственности остатка.

2 Планируемые результаты

- обосновывать делимость целых чисел;
- находить частные и остатки, включая случай отрицательного делимого;
- определять кратные на отрезке и уменьшать вычисления многочлена;
- шифровать и восстанавливать сообщение с помощью остатков;
- сопоставлять ручное решение с программной проверкой.

3 Программное обеспечение

Для приведённых примеров достаточно Python 3 и любой доступной среды для его запуска. Дополнительные пакеты не нужны. Ручное решение и математическое обоснование выполняются до программной проверки.

4 Методические сведения перед выполнением

4.1 Деление с остатком

Для целого a и положительного целого b требуется найти целые q, r:

$$a = bq + r, \qquad 0 \le r < b.$$

Удобная формула: $q = \lfloor a/b \rfloor, r = a - bq$. При ручном вычислении можно найти два соседних кратных b, между которыми находится a. Левое кратное равно bq, расстояние до a равно r.

Порядок решения задачи о делении с остатком

1. Убедиться, что делитель положителен.
2. Найти целое q, удовлетворяющее $bq \le a < b(q+1)$.
3. Вычислить $r = a - bq$.
4. Проверить восстановление исходного числа и обе границы остатка.
5. Сделать вывод о делимости: $b \mid a$ тогда и только тогда, когда $r = 0$.

4.2 Положительное и отрицательное число

Пусть $a = 173$ и $b = 12$. Ближайшие кратные: $12 \cdot 14 = 168$ и $12 \cdot 15 = 180$. Поэтому

$$173 = 12 \cdot 14 + 5, \qquad q = 14, \quad r = 5.$$

Для противоположного числа выбирается кратное слева:

$$-180 \le -173 < -168, \qquad -173 = 12(-15) + 7.$$

Получаем $q = -15, r = 7$. Равенство $-173 = 12(-14) - 5$ не является требуемым представлением, потому что -5 выходит за допустимый диапазон остатка.

Если исходное число кратно делителю, оба остатка равны нулю: $144 = 12 \cdot 12 + 0$ и $-144 = 12(-12) + 0$. Правило «для отрицательного числа взять $b - r$» применяется только при $r > 0$.

4.3 Кратные на целочисленном отрезке

Найдём все кратные 7 на отрезке $[-17,38]$. Пусть $x = 7t$. Тогда

$$-17 \le 7t \le 38 \quad \Leftrightarrow \quad -2 \le t \le 5, \qquad t \in \mathbb{Z}.$$

Следовательно, ответ равен $-14, -7, 0, 7, 14, 21, 28, 35$. Нуль включается, так как делится на 7. Количество чисел равно $5 - (-2) + 1 = 8$. В общем случае применяют границы $\lceil L/b \rceil$ и $\lfloor U/b \rfloor$; если нижняя больше верхней, кратных на отрезке нет.

4.4 Остаток многочлена

Для $a = 53$ и $b = 9$ найдём

$$R = \mathrm{rem}_9(a^2 + 3a + 5).$$

Сначала вычислим $r = \mathrm{rem}_9(53) = 8$. Затем уменьшим многочлен:

$$R = \mathrm{rem}_9(8^2 + 3 \cdot 8 + 5) = \mathrm{rem}_9(93) = 3.$$

После подстановки остатка результат также нужно привести по модулю: число 93 не является окончательным остатком. Независимая проверка даёт $53^2 + 3 \cdot 53 + 5 = 2973 = 9 \cdot 330 + 3$.

4.5 Шифр сдвига

Используем латинский алфавит A–Z и коды от 0 до 25. При $k = 5$ зашифруем слово CODE, коды которого равны 2,14,3,4:

$$2 \mapsto 7, \qquad 14 \mapsto 19, \qquad 3 \mapsto 8, \qquad 4 \mapsto 9.$$

Получаем HTIJ. Для восстановления кода из шифртекста вычитают ключ и берут неотрицательный остаток по модулю 26. Например, для кода 7 получаем $\mathrm{rem}_{26}(7 - 5) = 2$, то есть C.

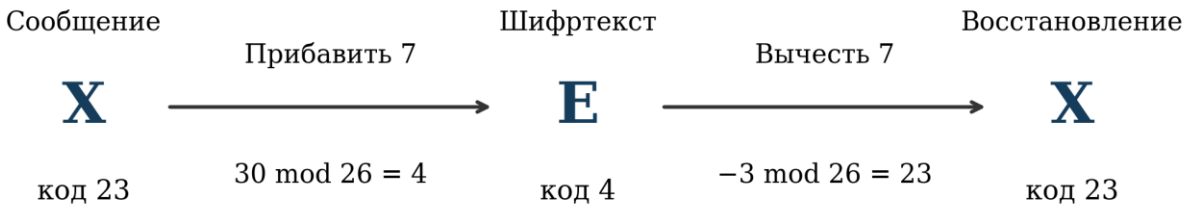


Рисунок 1. Шифрование и восстановление буквы X при ключе 7.

4.6 Доказательство делимости

Пусть $b \mid u$ и $b \mid v$. Тогда существуют целые s, t с $u = bs$, $v = bt$. Отсюда $5u - 3v = b(5s - 3t)$, поэтому $b \mid 5u - 3v$. Подстановка нескольких чисел может проверить пример, но не заменяет доказательства утверждения для всех целых u, v.

Во всех заданиях необходимо показывать ход решения. Итоговое число без объяснения не позволяет проверить, использовались ли верные свойства.

5 Программные примеры

5.1 Арифметические задачи

Для запуска достаточно Python 3; дополнительные пакеты не нужны. Сохраните следующий блок в файл `arithmetic_check.py` и запустите его в своей среде Python. Сначала получите указанные ниже результаты, затем подставляйте данные своего варианта. Каждый программный блок в методичке можно запускать отдельно.

Функция `divmod(a, b)` возвращает пару «неполное частное, остаток». При положительном целом `b` операция `//` округляет частное вниз, а `%` даёт неотрицательный остаток. Поэтому для отрицательного делимого нельзя заменять `a // b` выражением `int(a / b)`; кроме того, деление `/` переводит вычисление в вещественный тип.

```
def division_check(a, b):
    if b <= 0:
        raise ValueError("b must be positive")
    q, r = divmod(a, b)
    assert a == b * q + r
    assert 0 <= r < b
    return q, r

for a in (173, -173, 0):
    q, r = division_check(a, 12)
    print(a, q, r)

L, U, b = -17, 38, 7
t_min = -(-L // b)
t_max = U // b
multiples = [b * t for t in range(t_min, t_max + 1)]
print(multiples)

a, b = 53, 9
r = a % b
R = (r * r + 3 * r + 5) % b
assert R == (a * a + 3 * a + 5) % b
print(R)
```

Ожидаемый вывод

```
173 14 5
-173 -15 7
0 0 0
[-14, -7, 0, 7, 14, 21, 28, 35]
3
```

В первых трёх строках напечатаны a, q, r. Список содержит все кратные 7 на отрезке $[-17, 38]$, а последняя строка — остаток многочлена. Выражение `-(-L // b)` реализует $\lceil L/b \rceil$. Верхняя граница в `range` не включается, поэтому к `t_max` прибавлена единица. Если `t_min > t_max`, получится пустой список.

Проверки `assert` должны завершаться без сообщения об ошибке. Они сопоставляют конкретные вычисления с условиями задачи; доказательство общего свойства выполняется отдельно. При проверке своего варианта заменяйте соответствующие наборы исходных данных, а не только первое значение `a` в программе.

5.2 Шифр сдвига

В следующем примере используются заглавные латинские буквы A–Z. Команда `ord(ch) - ord("A")` переводит букву в число от 0 до 25. Затем к числу прибавляется ключ, результат приводится по модулю 26 и возвращается в буквенный вид с помощью `chr`. Для расшифрования используется та же функция с противоположным ключом.

Сохраните блок в файл `shift_check.py`. В начале функции проверяется алфавит: пробелы, строчные и кириллические буквы в этом учебном примере не допускаются.

```
def shift(text, key):
    if any(not ("A" <= ch <= "Z") for ch in text):
        raise ValueError("Use uppercase letters A-Z")
    result = []
    for ch in text:
        m = ord(ch) - ord("A")
        c = (m + key) % 26
        result.append(chr(ord("A") + c))
    return "".join(result)

plain, key = "CODE", 5
encrypted = shift(plain, key)
restored = shift(encrypted, -key)
print(encrypted)
print(restored)
assert restored == plain
```

Ожидаемый вывод

```
HTIJ
CODE
```

Для задания 4 замените `plain` на `"MATH"`, а `key` — на ключ своего варианта. Сначала вручную выпишите коды четырёх букв, затем сопоставьте их с программным результатом. Проверка `restored == plain` подтверждает обратное восстановление выбранного сообщения. Общая корректность формулы доказана в лекции; стойкость шифра этой проверкой не устанавливается.

6 Порядок выполнения работы

1. Изучить методические сведения и разобрать приведённые примеры.
2. Получить у преподавателя номер варианта и выписать исходные данные из раздела 8.
3. Выполнить задания 1–5 с ручными вычислениями и обоснованиями.
4. Проверить равенства, границы остатков и обратное восстановление сообщения. Для самостоятельной программной проверки подставить данные варианта в примеры кода.
5. Оформить решение по требованиям раздела 9 и подготовить ответы на контрольные вопросы.

7 Индивидуальные задания

Номер варианта назначает преподаватель. Значения a, b, L, U, k приведены в разделе 8. Во всех вариантах $a > 0$, $b > 0$, а отрезок включает оба конца.

Задание 1. Деление с остатком и делимость

Для чисел a и $-a$ найдите неполные частные и остатки при делении на b. Запишите оба равенства, проверьте диапазоны остатков и определите, делит ли b число a. Поясните, как из результата для a получить результат для $-a$.

Задание 2. Все кратные на отрезке

Выпишите все целые $x \in [L, U]$, для которых $b \mid x$. Укажите первое кратное, последнее кратное и их общее количество. Подтвердите, что ближайшее предыдущее и ближайшее следующее кратные лежат вне отрезка.

Задание 3. Уменьшение вычислений

Найдите остаток R числа $a^2 + 3a + 5$ при делении на b. Сначала замените a его остатком r, затем вычислите остаток $r^2 + 3r + 5$. Выполните независимую проверку прямым вычислением исходного выражения.

Задание 4. Проверка учебного шифрования

Зашифруйте слово МАТН ключом k своего варианта. Коды букв М, А, Т, Н равны соответственно 12,0,19,7. Для каждого символа вычислите

$$c = \mathrm{rem}_{26}(m + k).$$

Запишите числовой и буквенный шифртекст. Затем расшифруйте полученные четыре кода по формуле $m = \mathrm{rem}_{26}(c - k)$ и проверьте восстановление исходного слова. В этом задании модуль всегда равен 26; параметр b относится к заданиям 1–3.

Задание 5. Доказательство и контрпример

Докажите, что $b \mid u$ и $b \mid v$ влекут $b \mid 5u - 3v$ для любых целых u, v. Затем опровергните общее утверждение «из $d \mid uv$ следует $d \mid u$ или $d \mid v$», самостоятельно выбрав ненулевое d и целые u, v. Для контрпримера не требуется использовать параметры варианта.

Дополнительный вопрос. Почему преобразование $F(m) = \mathrm{rem}_{26}(2m)$ не позволяет однозначно расшифровать все сообщения? Сравните результаты для $m = 0$ и $m = 13$.

8 Варианты индивидуальных заданий

Вариант	a	b	L	U	k
1	164	8	-21	21	11
2	201	9	-22	22	18
3	238	10	-23	23	25
4	275	11	-24	24	7
5	312	12	-25	25	14
6	349	13	-26	26	21
7	386	14	-27	27	3
8	423	15	-28	28	10
9	460	7	-29	29	17
10	497	8	-30	30	24
11	534	9	-31	31	6
12	571	10	-32	32	13
13	608	11	-33	33	20
14	645	12	-34	34	2
15	682	13	-35	35	9
16	719	14	-36	36	16
17	756	15	-37	37	23
18	793	7	-38	38	5
19	830	8	-39	39	12
20	867	9	-40	40	19

9 Требования к отчёту

В решении указываются номер варианта и исходные данные. Для каждого задания приводятся вычисления, проверка и краткий вывод. Для задания 5 требуется буквенное доказательство, а для контрпримера — проверка всех его условий.

10 Критерии оценивания

Составляющая работы	Баллы
Задание 1 — два представления и проверка остатков	2
Задание 2 — список кратных и обоснование границ	2
Задание 3 — уменьшение выражения и независимая проверка	2
Задание 4 — шифрование и обратное восстановление	2
Задание 5 — доказательство и корректный контрпример	2
Максимум	10

Шкала относится к данной работе. Перенос результата в общую систему оценивания дисциплины выполняется по принятому в курсе порядку. Дополнительный вопрос и программная часть используются для обсуждения и самостоятельного углубления.

11 Контрольные вопросы

1. Какие равенство и границы нужно проверить после нахождения q, r?
2. Почему для -173 при делении на 12 получаем частное -15, а не -14?
3. Когда остатки a и $-a$ оба равны нулю?
4. Почему в `range(t_min, t_max + 1)` нужна единица?
5. Почему перед вычислением многочлена можно заменить число его остатком?
6. Как связаны прибавление ключа и применение противоположного ключа?

Литература

Мартынов, 2020, глава 3; Kraft–Washington, 2018, §§2.1 и 2.5 из предоставленного фрагмента; Paar–Pelzl, 2010, глава 1. Определения и доказательства — в лекции 1.